|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **INSTITUTO TECNOLÓGICO DE LA PAZ**  ING.EN SISTEMAS COMPUTACIONALES | | **sistemas** | |
| **Manual de Prácticas de la Materia:**  **Seguridad en infraestructura Web** | **Unidad:**  **III** |
| **Equipo: Alfonso Delgado Aguirre, Marco Antonio Suastegui Valtierra, Victor Daniel García Lemus.** | | **Fecha: 30/10/19** | | **Grupo: H** |

|  |  |
| --- | --- |
| **No. Práctica: 2** | **Título de la Práctica: DETECCIÓN DE VULNERABILIDADES** |
| **Competencias:** | |
| **Objetivo:** Determinar los riesgos a los que están expuestos un activo informático. | |

***Marco teórico:***

**WordPress**

Es un sistema de gestión de contenidos lanzado el 27 de mayo de 2003, enfocado a la creación de cualquier tipo de página web. Originalmente alcanzó una gran popularidad en la creación de blogs, para convertirse con el tiempo en una de las principales herramientas para la creación de páginas web comerciales. Está desarrollado en el lenguaje PHP para entornos que ejecuten MySQL y Apache, bajo licencia GPL y es software libre.

**FreeBSD**

FreeBSD es un sistema operativo open source para computadoras basado en las CPU de arquitectura x86, Intel 80386, Intel 80486 (versiones SX y DX), y Pentium. También funciona en procesadores compatibles con x86 como AMD y Cyrix. En la actualidad se ejecuta en once arquitecturas distintas​ como, Alpha, AMD64, IA-64, MIPS, PowerPC y UltraSPARC.

FreeBSD está basado en la versión 4.4 BSD-Lite del Computer Systems Research Group (CSRG) de la Universidad de Berkeley en California.

**Programas utilizados**

**Sparty**

Sparty es una herramienta de código abierto escrita en python para auditar aplicaciones web usando sharepoint y arquitectura de portada. La motivación detrás de esta herramienta es proporcionar una manera fácil y robusta de analizar las configuraciones de seguridad de las aplicaciones web basadas en sharepoint y en portada. Debido a la naturaleza compleja de este software de administración web, se requiere tener una herramienta simple y eficiente que recopile información, verifique los permisos de acceso, descargue información crítica de los archivos predeterminados y realice una explotación automatizada si se identifican riesgos de seguridad. Varios escáneres automáticos no alcanzan esto y Sparty es una solución para eso.

**Nmap**

Nmap es un programa de código abierto que sirve para efectuar rastreo de puertos escrito originalmente por Gordon Lyon y cuyo desarrollo se encuentra hoy a cargo de una comunidad. Fue creado originalmente para Linux aunque actualmente es multiplataforma.

***Recursos y/o Materiales:***

* Navegador Google Chrome
* Computadoras

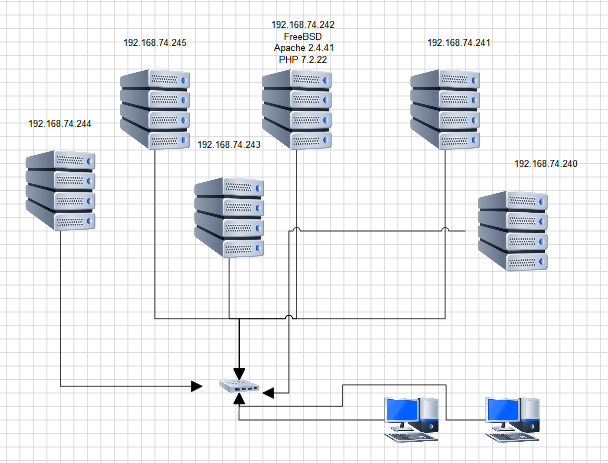
***Procedimiento:***

Se utiliza una herramienta de escáner de vulnerabilidades. Con el objetivo de detectar los potenciales riesgos al que están expuestos los equipos seleccionados, debido a que estos juegan el rol más crítico para la red.

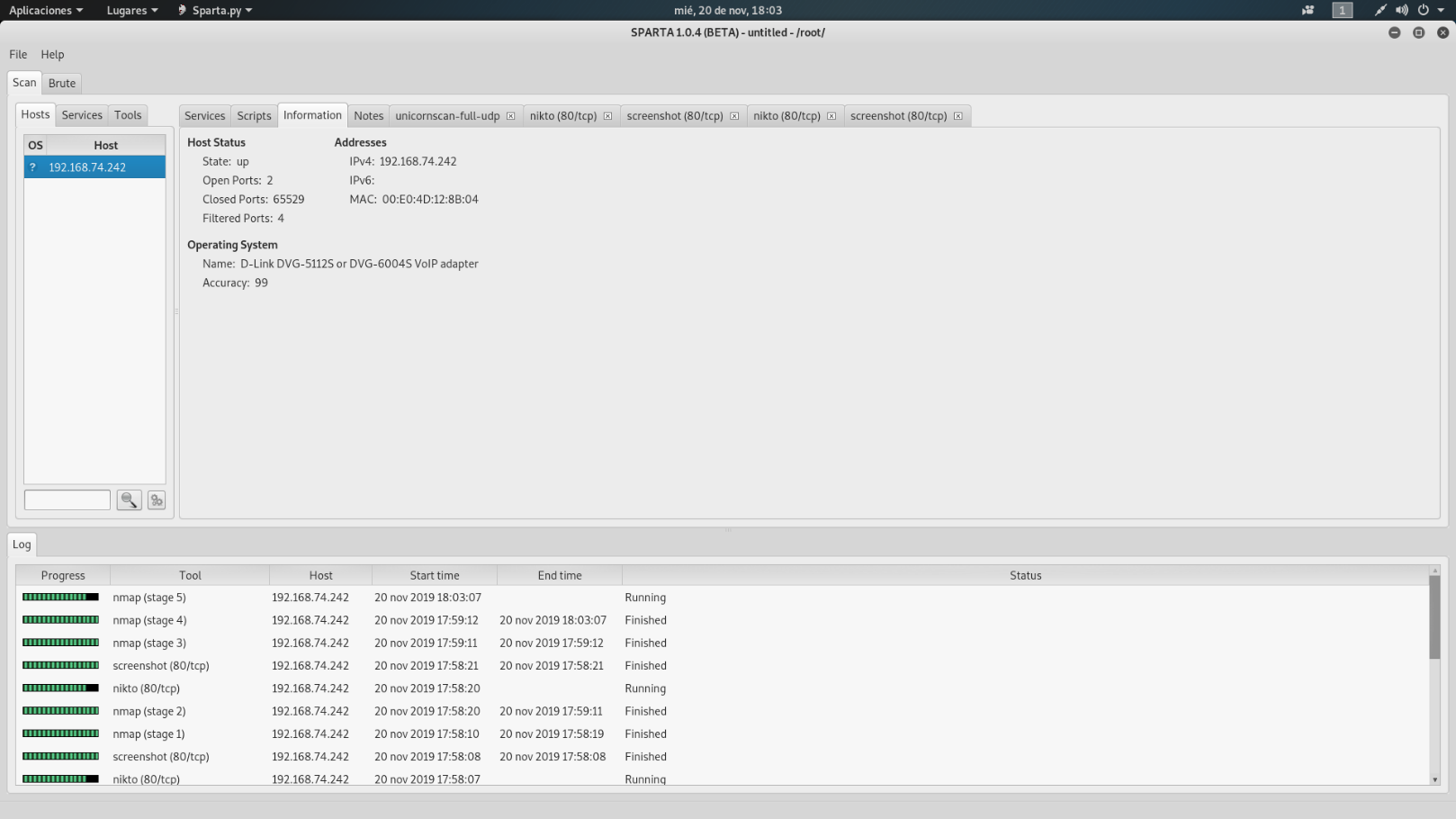
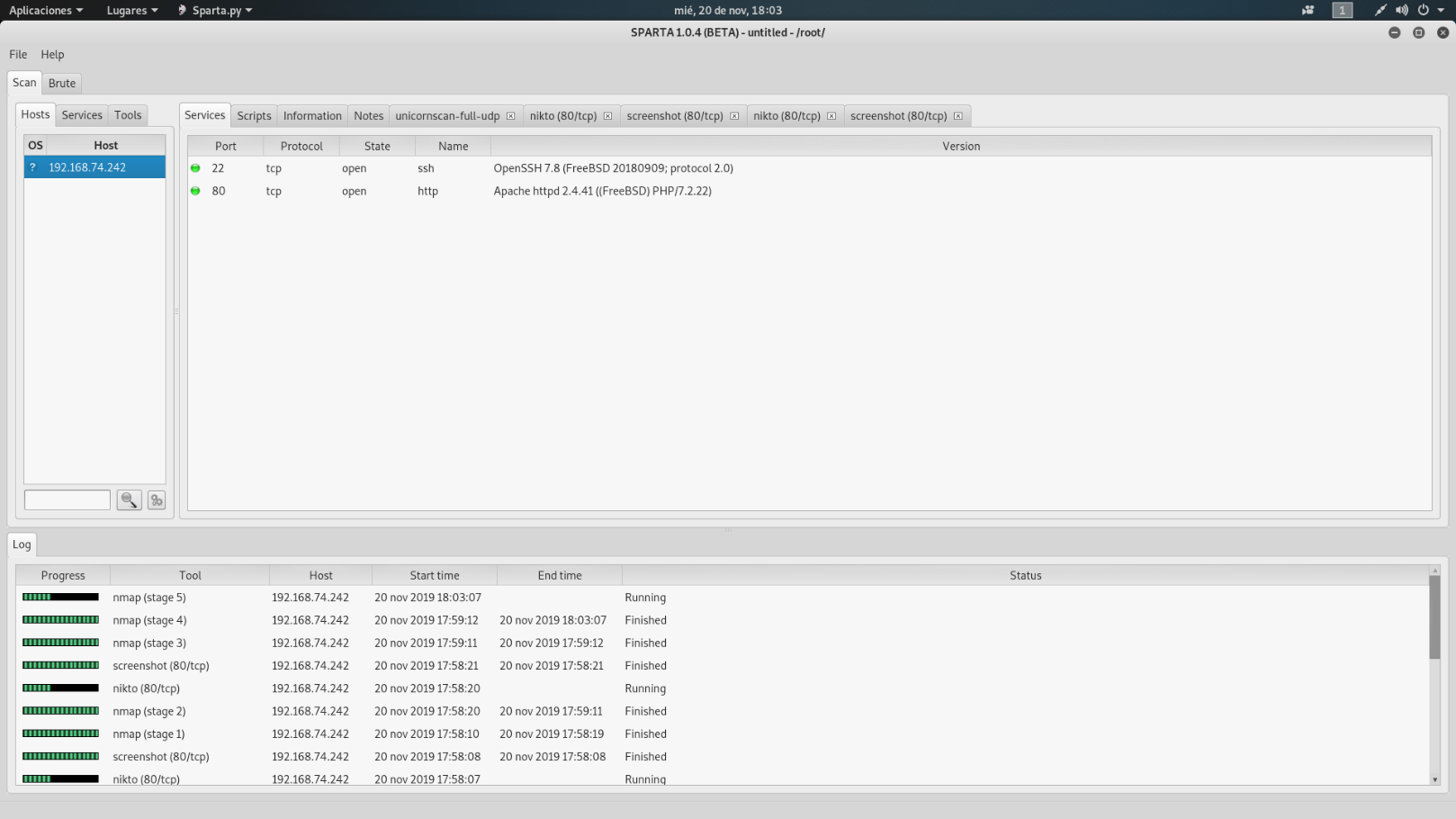
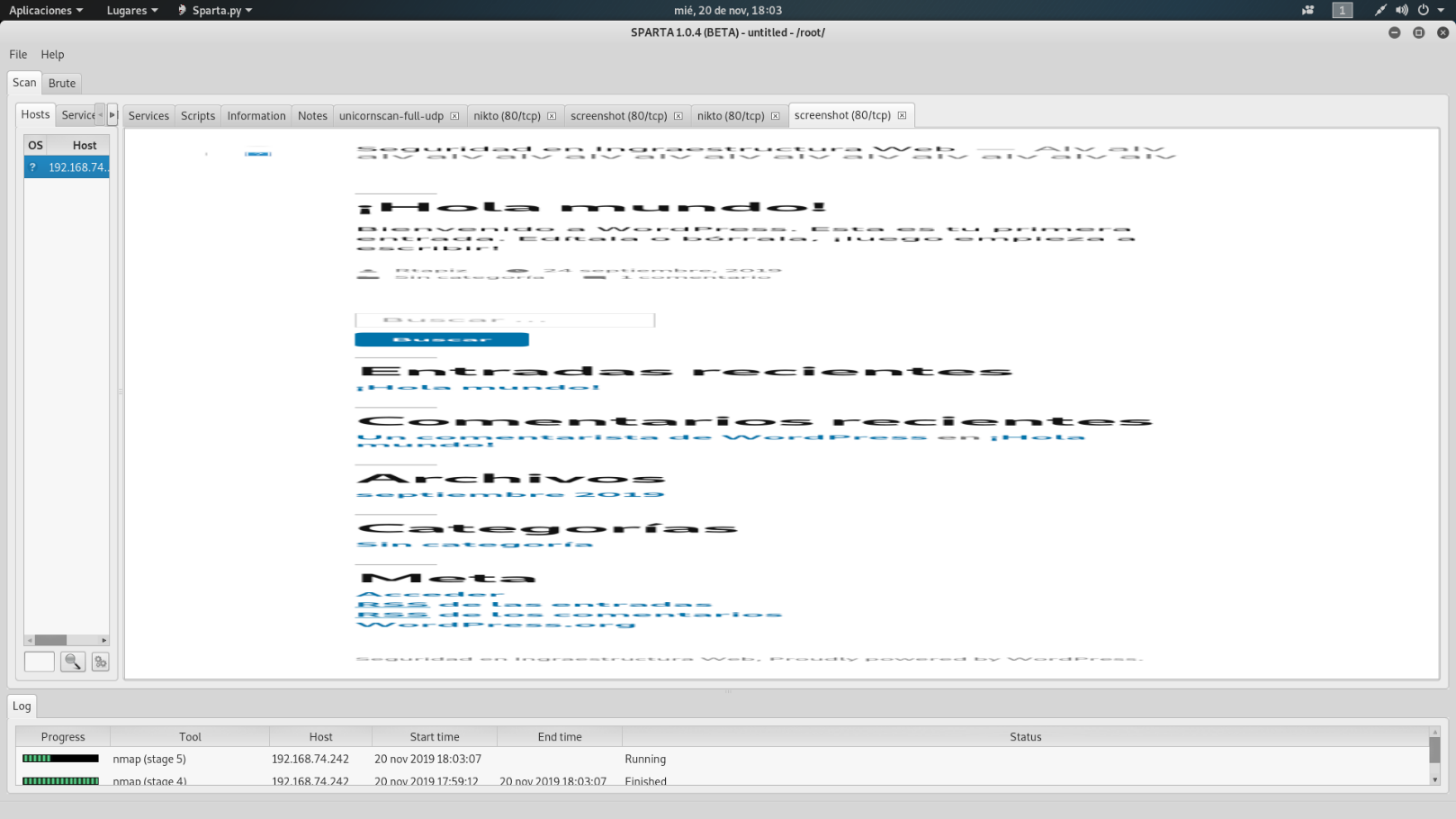
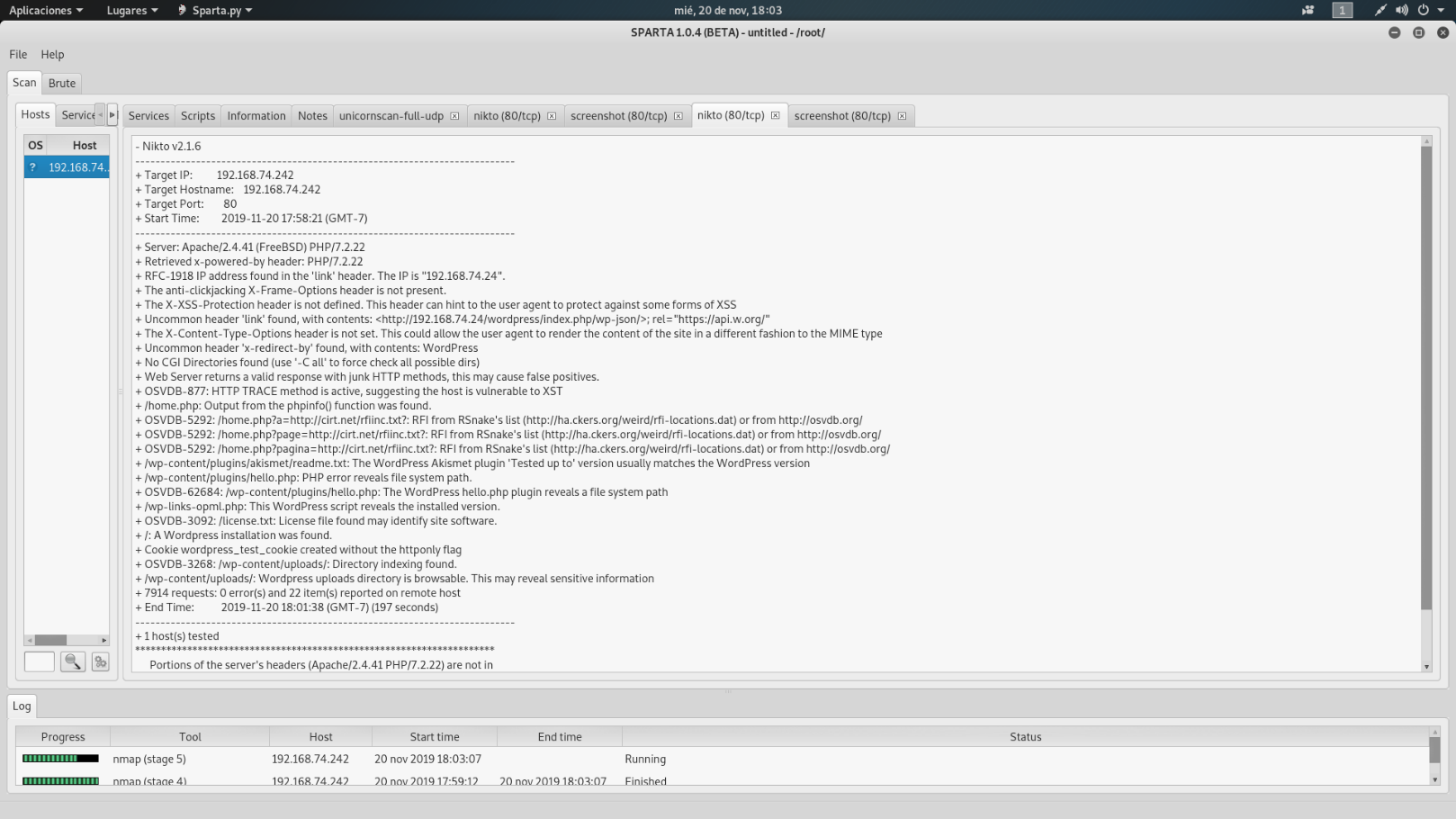
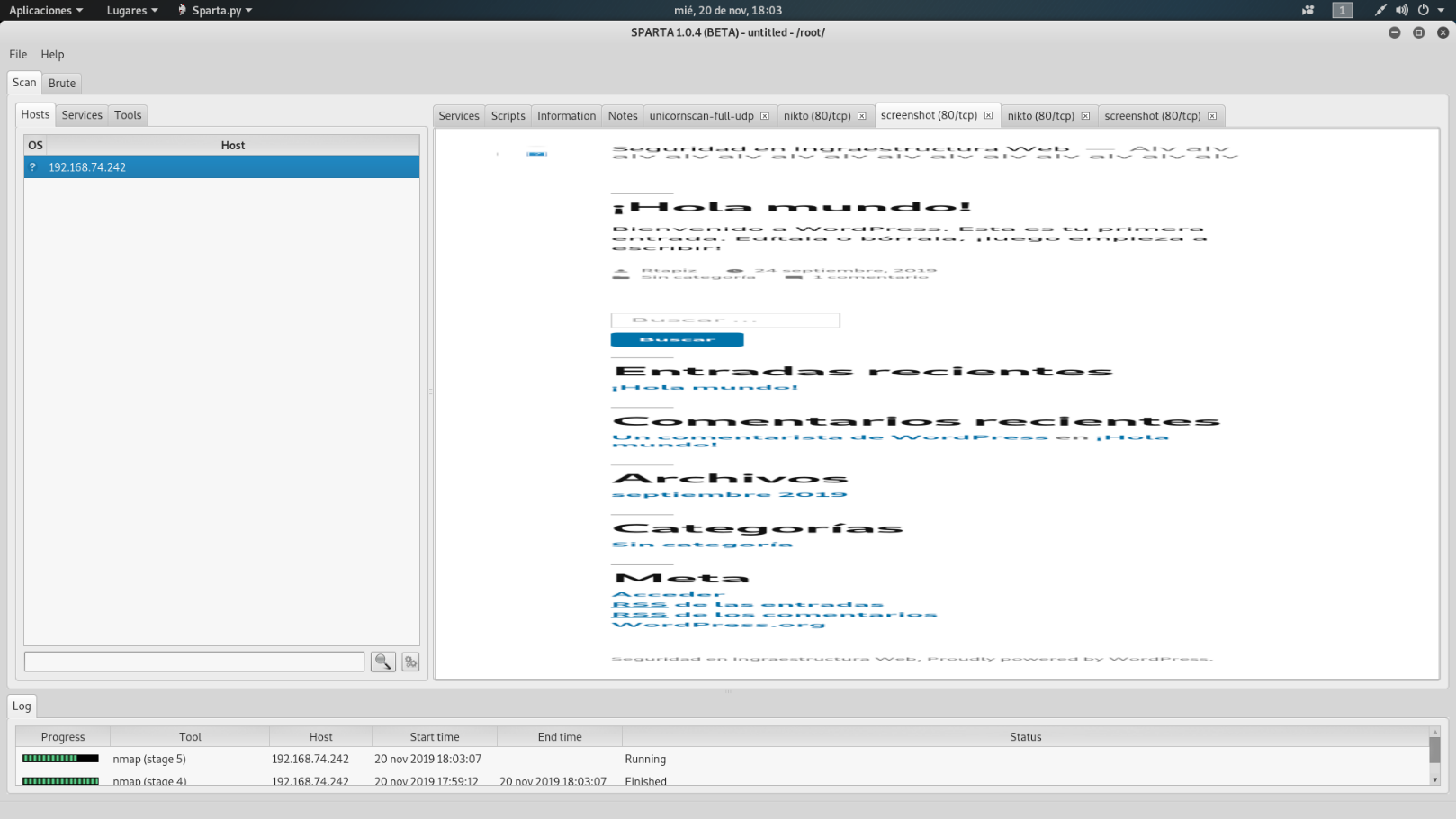
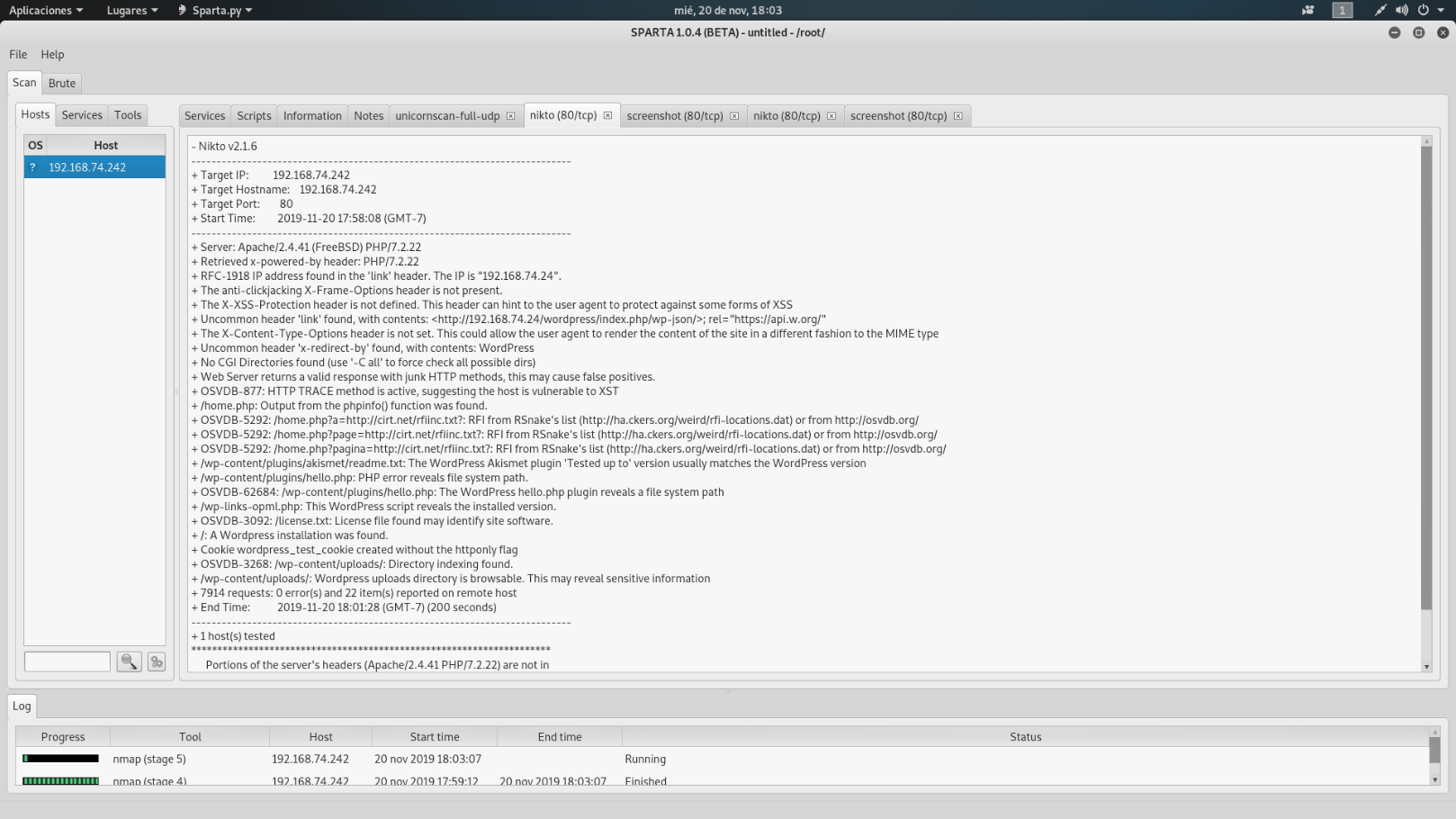
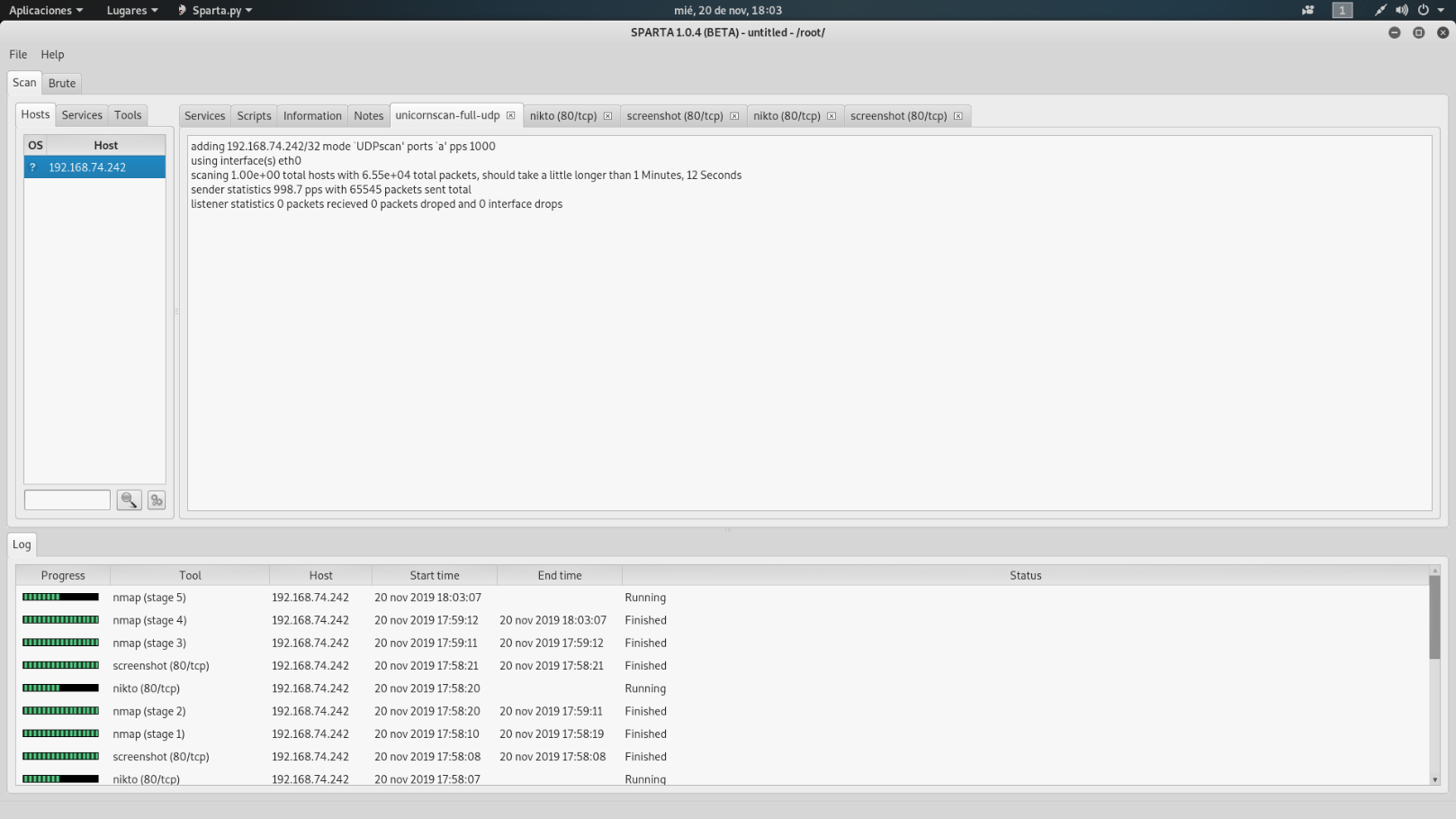
***Red, IP, Topología***

**Dirección IP: 192.168.74.242**

* Dirección IP: 192.168.74.242
* Sistema Operativo: FreeBSD
* Apache 2.4.41
* PHP 7.2.22
* *Fase 3(Escaneos)*



**Sparty**



**Nmap**

root@kali:~# nmap -v -A 192.168.74.242

Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-20 17:16 MST

NSE: Loaded 151 scripts for scanning.

NSE: Script Pre-scanning.

Initiating NSE at 17:16

Completed NSE at 17:16, 0.00s elapsed

Initiating NSE at 17:16

Completed NSE at 17:16, 0.00s elapsed

Initiating NSE at 17:16

Completed NSE at 17:16, 0.00s elapsed

Initiating ARP Ping Scan at 17:16

Scanning 192.168.74.242 [1 port]

Completed ARP Ping Scan at 17:16, 0.05s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 17:16

Completed Parallel DNS resolution of 1 host. at 17:16, 0.30s elapsed

Initiating SYN Stealth Scan at 17:16

Scanning 192.168.74.242 [1000 ports]

Discovered open port 22/tcp on 192.168.74.242

Discovered open port 80/tcp on 192.168.74.242

Increasing send delay for 192.168.74.242 from 0 to 5 due to max\_successful\_tryno increase to 4

Completed SYN Stealth Scan at 17:16, 5.92s elapsed (1000 total ports)

Initiating Service scan at 17:16

Scanning 2 services on 192.168.74.242

Completed Service scan at 17:16, 6.39s elapsed (2 services on 1 host)

Initiating OS detection (try #1) against 192.168.74.242

Retrying OS detection (try #2) against 192.168.74.242

Retrying OS detection (try #3) against 192.168.74.242

Retrying OS detection (try #4) against 192.168.74.242

Retrying OS detection (try #5) against 192.168.74.242

NSE: Script scanning 192.168.74.242.

Initiating NSE at 17:16

Completed NSE at 17:16, 8.26s elapsed

Initiating NSE at 17:16

Completed NSE at 17:16, 0.76s elapsed

Initiating NSE at 17:16

Completed NSE at 17:16, 0.00s elapsed

Nmap scan report for 192.168.74.242

Host is up (0.00018s latency).

Not shown: 998 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.8 (FreeBSD 20180909; protocol 2.0)

| ssh-hostkey:

| 2048 ac:32:3e:09:0d:f9:2e:89:36:23:8c:c9:99:5b:ee:fd (RSA)

| 256 1b:97:9a:9b:04:e9:26:0f:39:01:7c:b8:bf:43:87:63 (ECDSA)

|\_ 256 d0:be:6d:6e:39:e9:f1:fb:fa:3c:0a:2e:d3:33:da:35 (ED25519)

80/tcp open http Apache httpd 2.4.41 ((FreeBSD) PHP/7.2.22)

|\_http-generator: WordPress 5.2.3

| http-methods:

|\_ Supported Methods: GET HEAD POST OPTIONS

|\_http-server-header: Apache/2.4.41 (FreeBSD) PHP/7.2.22

|\_http-title: Seguridad en Ingraestructura Web &#8211; Alv alv alv alv alv a...

MAC Address: 00:E0:4D:12:8B:04 (Internet Initiative Japan)

No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).

TCP/IP fingerprint:

OS:SCAN(V=7.80%E=4%D=11/20%OT=22%CT=1%CU=34657%PV=Y%DS=1%DC=D%G=Y%M=00E04D%

OS:TM=5DD5D767%P=x86\_64-pc-linux-gnu)SEQ(SP=102%GCD=1%ISR=10C%TI=Z%CI=Z%II=

OS:RI%TS=21)OPS(O1=M5B4NW6ST11%O2=M5B4NW6ST11%O3=M5B4NW6NNT11%O4=M5B4NW6ST1

OS:1%O5=M5B4NW6ST11%O6=M5B4ST11)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF

OS:%W6=FFFF)ECN(R=Y%DF=Y%T=40%W=FFFF%O=M5B4NW6SLL%CC=Y%Q=)T1(R=Y%DF=Y%T=40%

OS:S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=Y%DF=Y%T=40%W=FFFF%S=O%A=S+%F=AS%O=M5B

OS:4NW6ST11%RD=0%Q=)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y

OS:%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%R

OS:D=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IP

OS:L=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=S%T=40%CD=S)

Uptime guess: 0.000 days (since Wed Nov 20 17:16:27 2019)

Network Distance: 1 hop

TCP Sequence Prediction: Difficulty=255 (Good luck!)

IP ID Sequence Generation: All zeros

Service Info: OS: FreeBSD; CPE: cpe:/o:freebsd:freebsd

TRACEROUTE

HOP RTT ADDRESS

1 0.18 ms 192.168.74.242

NSE: Script Post-scanning.

Initiating NSE at 17:16

Completed NSE at 17:16, 0.00s elapsed

Initiating NSE at 17:16

Completed NSE at 17:16, 0.00s elapsed

Initiating NSE at 17:16

Completed NSE at 17:16, 0.00s elapsed

Read data files from: /usr/bin/../share/nmap

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 33.61 seconds

Raw packets sent: 1429 (66.670KB) | Rcvd: 1076 (46.586KB)

Conclusiones

Con ayuda de las aplicaciones utilizadas para el análisis de vulnerabilidades detectamos las siguientes vulnerabilidades:

|  |  |
| --- | --- |
| Vulnerabilidades | Descripción |
| Retrieved x-power-by header: PHP/7.2.2.22 | x / Patrón y patrones relacionados, que permite a los atacantes remotos atacar y ejecutar código PHP arbitrario a través de un encabezado HTTP diseñado, Comandos SQL arbitrarios a través de un comentario que se maneja mal después de la recuperación de la papelera. |
| RFC-1918 ip address found in the link header. The IP is “192.168.74.24” | Dirección IP RFC-1918 encontrada en el encabezado del enlace. La IP es "192.168.74.24" |
| The anti-clickjacking X-Frame- Options Header is no present. | El encabezado de opciones X-Frame-anti-clickjacking no está presente. Es cuando un atacante usa múltiples capas transparentes u opacas para engañar a un usuario para que haga clic en un botón o enlace en otra página cuando tenía la intención de hacer clic en la página de nivel superior. |
| The X-Content-Type-Options header is not set. | El encabezado X-Content-Type-Options no está configurado. Esto podría permitir que el agente de usuario presente el contenido del sitio de una manera diferente al tipo MIME.  El encabezado HTTP de respuesta X-Content-Type-Options es un marcador utilizado por el servidor para indicar que los tipos MIME anunciados en los encabezados Content-Type no deben cambiarse y seguirse. Esto permite optar por la inhalación de tipo MIME o, en otras palabras, es una forma de decir que los webmasters sabían lo que estaban haciendo. |
| No CGI | Directorios encontrados (use '-C all' para forzar la verificación de todos los directorios posibles). |
| Web server return a valid response with junk HTTP methods, this may cause false positives | El servidor web devuelve una respuesta válida con métodos HTTP basura, esto puede causar falsos positivos. |
| OSVDB-877: | HTTP TRACER method is active, suggesting the host is vulnerable to XST.  El método HTTP TRACER está activo, lo que sugiere que el host es vulnerable a XST.  Un ataque de rastreo entre sitios (XST) implica el uso de secuencias de comandos entre sitios (XSS) y los métodos HTTP TRACE o TRACK. Según RFC 2616 , "TRACE permite al cliente ver lo que se recibe en el otro extremo de la cadena de solicitud y usar esos datos para pruebas o información de diagnóstico", el método TRACK funciona de la misma manera pero es específico para el IIS de Microsoft Servidor web. XST podría usarse como un método para robar las cookies de los usuarios a través de Cross-site Scripting (XSS) incluso si la cookie tiene establecido el indicador " HttpOnly " y / o expone el encabezado de autorización del usuario. |
| OSVDB-5292 | osvdb-5292: /home.php?a=http://cirt.net/rfiinc.txt? RFI from RSnake's list (http://ha.ckers.org/weird/rfi-locations.dat) ot from <http://osvdb.org/>)  Local File Inclusion (LFI) o, en español, Inclusión local de archivos.  Esta técnica consiste en incluir ficheros locales, es decir, archivos que se encuentran en el mismo servidor de la web con este tipo de fallo -a diferencia de Remote File Inclusión o inclusión de archivos remotos (RFI) que incluye archivos alojados en otros servidores. Esto se produce como consecuencia de un fallo en la programación de la página, filtrando inadecuadamente lo que se incluye al usar funciones en PHP para incluir archivos. |
| OSVDB-5292 | osvdb-5292: /home.php?page=http://cirt.net/rfiinc.txt? RFI from RSnake's list (http://ha.ckers.org/weird/rfi-locations.dat) ot from http://osvdb.org/) |
| OSVDB-5292 | osvdb-5292: /home.php?pagina=http://cirt.net/rfiinc.txt? RFI from RSnake's list (http://ha.ckers.org/weird/rfi-locations.dat) ot from http://osvdb.org/) |
| OSVDB-62684 | /wp-content/plugins/hello.php: el complemento hello.php de WordPress revela una ruta del sistema de archivos |
| OSVDB-3092 | /licese.txt El archivo de licencia encontrado puede identificar el software del sitio. |
| OSVDB-3268 | / wp-content / uploads /: indexación de directorio encontrada. |